

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Atsushi HAMANO

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: DATA SENDING/RECEIVING SYSTEM FOR ENABLING DoS COUNTERMEASURE

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-016641	January 24, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)  
☐ are submitted herewith  
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
\_\_\_\_\_  
Bradley D. Lytle

Registration No. 40,073

C. Irvin McClelland  
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   1 月 2 4 日  
Date of Application:

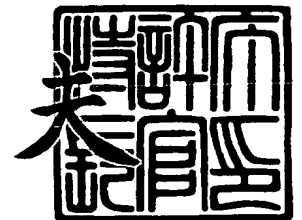
出 願 番 号            特 願 2 0 0 3 - 0 1 6 6 4 1  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 0 1 6 6 4 1 ]

出      願      人            ソニー株式会社  
Applicant(s):

2 0 0 3 年 1 1 月 1 9 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 0290767904

【提出日】 平成15年 1月24日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G09C 1/00

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号ソニー株式会社内

    【氏名】 濱野 淳史

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

【代理人】

    【識別番号】 100082740

    【弁理士】

    【氏名又は名称】 田辺 恵基

【手数料の表示】

    【予納台帳番号】 048253

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9709125

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信装置及び受信装置

【特許請求の範囲】

【請求項 1】

所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信する送信手段と、

上記送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各上記送信パケットに付加する識別情報付加手段と

を具えることを特徴とする送信装置。

【請求項 2】

上記識別情報生成手段は、

上記送信パケットの送り出し方向に未符号化状態で上記識別情報を付加することを特徴とする請求項 1 に記載の送信装置。

【請求項 3】

上記識別情報は、

所定の擬似乱数と、当該擬似乱数に固有のシーケンス番号情報とでなることを特徴とする請求項 1 に記載の送信装置。

【請求項 4】

所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信する第 1 のステップと、

上記送信パケットの受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各上記送信パケットに付加する第 2 のステップと

を具えることを特徴とする送信方法。

【請求項 5】

送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信する受信手段と、

上記受信手段が受信した各上記送信パケットのうち、当該パケットの内容が変更された上記送信パケットである内容変更パケットを検出する検出手段と、

上記検出手段により検出された上記内容変更パケットの受信状況に応じて、上記検出手段だけに識別させるための識別情報の上記送信パケットへの付加を上記送信側に要求する要求手段と

を具えることを特徴とする受信装置。

#### 【請求項 6】

上記要求手段は、

上記内容変更パケットに係る上記送信パケットを送信する上記送信側に対してのみ上記識別情報の付加を要求する

ことを特徴とする請求項 6 に記載の受信装置。

#### 【請求項 7】

送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信する第 1 のステップと、

上記第 1 のステップで受信された各上記送信パケットのうち、当該パケットの内容が変更された上記送信パケットである内容変更パケットを検出する第 2 のステップと、

上記第 2 のステップで検出された上記内容変更パケットの受信状況に応じて、上記検出手段だけに識別させるための識別情報の上記送信パケットへの付加を上記送信側に要求する第 3 のステップと

を具えることを特徴とする受信方法。

#### 【発明の詳細な説明】

##### 【0 0 0 1】

#### 【発明の属する技術分野】

本発明は送信装置及び受信装置に関し、例えばインターネットを介して送信装置と受信装置とが接続されてなる送受信システムに適用して好適なものである。

##### 【0 0 0 2】

#### 【従来の技術】

従来、本出願人によって既に開示した特願2002-263272号に係る送受信システムは、送信側では送信対象の暗号パケットを送信する際に、受信装置だけに正当性を証明するための正当性証明情報を未暗号化状態で付加した後にインターネッ

トを介して送信し、一方受信側では当該暗号パケットに付加された正当性証明情報の正当性が維持されている判定結果が得られた場合にのみ暗号パケットを復号する。

#### 【0003】

従って送受信システムは、サービス妨害 (DoS:Denial of Service) 行為のうち、暗号パケットの送信元アドレス等を書き換えることにより生成された詐称パケットを大量に受信装置へ送信する行為があった場合、当該受信装置では第三者の知り得ない正当性証明情報に基づいて詐称パケットを復号する前に破棄することができ、かくして、大量の詐称パケットを受信した場合であっても迅速な処理を実現することができるようになされている。

#### 【0004】

##### 【発明が解決しようとする課題】

ところがかかる構成の送受信システムにおいては、サービス妨害行為の有無に係わらず常に正当性証明情報を暗号パケットに付加して送信することにより、当該サービス妨害行為がなかった場合におけるシステム全体の処理負荷が顕著に増大し、その結果、システム全体としての送信効率が悪化してしまうという問題があった。

#### 【0005】

本発明は以上の点に考慮してなされたもので、システム全体としての送信効率を向上し得る送信装置、送信方法、受信装置及び受信方法を提案しようとするものである。

#### 【0006】

##### 【課題を解決するための手段】

かかる課題を解決するため本発明においては、所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信し、当該送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各送信パケットに付加する。

#### 【0007】

この場合、受信側から要求があった期間以外については識別情報を各送信パケ

ットに付加しない分だけ送信手段、正当性付加手段及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができる。

#### 【0008】

また、かかる課題を解決するため本発明においては、送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信し、当該受信された各送信パケットのうち、当該パケットの内容が変更された送信パケットである内容変更パケットを検出し、当該検出した内容変更パケットの受信状況に応じて、検出手段だけに識別させるための識別情報の送信パケットへの付加を送信側に要求する。

#### 【0009】

この場合、送信側に要求しない際に送信側からは識別情報の付加された送信パケットが送信されない分だけ送信装置及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができる。

#### 【0010】

#### 【発明の実施の形態】

以下図面について、本発明の一実施の形態を詳述する。

#### 【0011】

##### (1) 全体構成

図1において、1は全体として本発明を適用した送受信システムを示し、送信装置2、受信装置3及び通信妨害装置4がインターネット5に接続されており、当該送信装置2と受信装置3とがインターネット5を介して各種データの授受を行い得るようになされている。

#### 【0012】

送信装置2は、送信対象データを所定長のデータ片に分割し、当該データ片に対して所定の通信プロトコルに従ってパケット暗号化処理を施し、その結果順次生成される送信パケットPK（PK1、PK2、……）を受信装置3へ送信する。

#### 【0013】

受信装置3は、送信装置2から送信される送信パケットPKを受信し、その送

信パケット P K に対して当該送信装置 2 と同一の通信プロトコルに従ってパケット復号処理を施し、その結果復元されるデータ片を例えば内部メモリ（図示せず）に記憶する。

【0014】

通信妨害装置 4 は、受信装置 3 に対してサービス妨害（DoS: Denial of Service）行為を行うようになされており、具体的には送信装置 2 から受信装置 3 へ送信される送信パケット P K（P K 1、P K 2、……）を監視し、当該送信中の送信パケット P K（P K 1、P K 2、……、又は P K n）を不当に入手し、当該入手した送信パケット P K の内容を変更した送信パケット（以下、これを内容変更パケットと呼ぶ）F P K を生成し、これを大量に複製した後に順次受信装置 3 へ送信する。

【0015】

ここで、受信装置 3 は、通信妨害装置 4 から送信される内容変更パケット F P K を大量に受信すると、サービス妨害行為に対する対策（以下、これをサービス妨害対策と呼ぶ）の開始を要求する要求データ D N a を生成し、これを送信装置 2 へ送信する。

【0016】

この場合、送信装置 2 は、受信装置 3 から送信される要求データ D N a を受信した以降に順次生成した送信パケット P K については、受信装置 3 だけに正当性を証明する識別情報をサービス妨害対策として付加し、その結果順次得られる送信パケット（以下、これを、妨害対策パケットと呼ぶ）B M P K（B M P K 1、B M P K 2……）を順次受信装置 3 へ送信する。

【0017】

受信装置 3 は、送信装置 2 から送信される妨害対策パケット B M P K 及び通信妨害装置 4 から送信される内容変更パケット F P K のうち、当該妨害対策パケット B M P K だけを復元し、その結果得られるデータ片を内部メモリ（図示せず）に記憶し得るようになされている。

【0018】

また受信装置 3 は、通信妨害装置 4 から送信される内容変更パケット F P K が



少なくなると、サービス妨害対策の停止を要求する要求データ D N b を生成し、これを送信装置 2 へ送信する。

#### 【0019】

この場合、送信装置 2 は、受信装置 3 から送信される要求データ D N b を受信すると、当該要求データ D N b を受信した以降に順次生成した送信パケット P K については識別情報を付加することなくそのまま受信装置 3 へ送信するようになされている。

#### 【0020】

このように送受信システム 1 は、受信装置 3 における内容変更パケット F P K の受信状況に応じて、要求データ D N (D N a、D N b) を介して識別情報 J P の付加の有無を要求することにより、当該内容変更パケット F P K の受信数が多い（すなわちサービス妨害行為の規模が大きい）場合にのみ、送信パケット P K に識別情報を付加した妨害対策パケット B M P K をインターネット 5 を介して送信装置 2 と受信装置 3 との間で送受信し得るようになされている。

#### 【0021】

なお、図 1 の実施の形態における送受信システム 1 においては、インターネット 5 を介して当該送信装置 2 と同一構成の 1 又は 2 以上の送信装置が受信装置 3 に接続されている場合、受信装置 3 は、当該複数の送信装置（送信装置 2 も含む。以下同じ）のうち、内容変更パケット F P K の生成元となった送信パケット P K を送信する送信装置 2 に対してのみ、要求データ D N (D N a、D N b) を介して識別情報 J P の付加の有無を要求し得るようになされている。

#### 【0022】

##### (2) 送信装置の構成

図 2 に示すように、パケット生成部 11 は、内部メモリから読み出した又は外部から供給された送信対象データ D 10 を所定長でなる複数のデータ片に分割し、当該データ片に対して例えば I P sec (Internet Protocol security) と呼ばれる通信プロトコルに従ってパケット暗号化処理を施すようになされている。

#### 【0023】

具体的にパケット生成部 11 は、I P sec で規定される複数の暗号鍵情報、暗

号化アルゴリズムや認証アルゴリズム等の各種セキュリティ情報群（S A (Security Association)）のうち、受信装置 3 へ最初にアクセスした際に送信装置 2 と受信装置 3 とのアドレスに基づいて予め決定しておいた使用する S A（以下、これを使用セキュリティと呼ぶ）に従ってデータ片を暗号化した後にヘッダを付加し、その結果順次生成される送信パケット P K（P K 1、P K 2、……）を送信処理部 1 2 に与える。

#### 【0024】

因みに、かかる送信パケット P K には、使用セキュリティを示す S P I (Security Parameter Index) と呼ばれるインデックス情報も含まれている。

#### 【0025】

送信処理部 1 2 の識別情報付加部 1 3 は、識別情報を付加しない第 1 のモード（以下、これを妨害対策停止モードと呼ぶ）である場合には、当該識別情報付加部 1 3 自身における処理を停止した休止状態となる。

#### 【0026】

従ってパケット生成部 1 1 から順次与えられる送信パケット P K（P K 1、P K 2、……）はそのままインターフェイス（以下、これを送信側インターフェイスと呼ぶ）1 5 を介して受信装置 3（図 1）へ送信される。

#### 【0027】

これに対して識別情報付加部 1 3 は、識別情報を付加する第 2 のモード（以下、これを妨害対策モードと呼ぶ）である場合、まず、図 3 に示すように、パケット生成部 1 1 から与えられる送信パケット P K（P K 1、P K 2、……）ごとに固有の識別情報 J P（J P 1、J P 2、……）を生成する。

#### 【0028】

次いで識別情報付加部 1 3 は、送信パケット P K の送り出し方向に未符号化状態で識別情報 J P を付加し、その結果順次生成される妨害対策パケット B M P K（B M P K 1、B M P K 2……）を送信側インターフェイス 1 5 を介して受信装置 3（図 1）へ送信する。

#### 【0029】

ここで、識別情報付加部 1 3 は、識別情報 J P の具体的な生成手法として、予

め内部メモリ（図示せず）に格納された I P sec の規定とは別に送信装置 2 と受信装置 3 とだけが独自に有する識別情報生成アルゴリズムにより、まずパケット生成部 11 で用いられた暗号化鍵情報に基づいて種情報（シード）を導出する。

#### 【0030】

次いで識別情報付加部 13 は、図 4 に示すように、種情報（シード）から通信妨害装置 4 には知り得ない固有の擬似乱数 G（G1、G2、……）を生成し、当該擬似乱数 G の生成順番に対応するシーケンシャルな番号のデータ（以下、これをシーケンス番号と呼ぶ）S（S1、S2、……）を当該擬似乱数 G の例えば先頭に付加することにより識別情報 JP（JP1、JP2、……）を生成する。

#### 【0031】

従って識別情報付加部 13 は、擬似乱数 G とシーケンス番号 S との対応関係を通信妨害装置 4 に対しては単に規則性のないデータ列として認識させ得るのみならず、当該擬似乱数 G とシーケンス番号 S との組み合わせが 2 度と同一の状態となることはない識別情報 JP（JP1、JP2、……）を生成することができ、かくして、を受信装置 3 に対してのみほぼ確実に識別させ得る信頼性の高い識別情報 JP として生成し得るようになされている。

#### 【0032】

また識別情報付加部 13 は、送信装置 2 と受信装置 3 とだけが独自に有する識別情報生成アルゴリズムに従って識別情報 JP を生成した後に未符号化状態で送信パケット PK に付加しているので、当該送信パケット PK の復号前に当該識別情報 JP を受信装置 3（図 1）に対してのみ認識させ得るようになされている。

#### 【0033】

送信処理部 12 のフィードバック受信部 14 は、受信装置 3（図 1）から送信される要求データ DN（DNa、DNb）を受信するようになされており、サービス妨害対策を開始させる要求データ DNa を受信した場合には、識別情報付加部 13 を妨害対策モードに遷移させる。

#### 【0034】

これに対してフィードバック受信部 14 は、サービス妨害対策を停止させる要求データ DNb を受信した場合には、識別情報付加部 13 を妨害対策停止モード

に遷移させる。

#### 【0035】

このように送信処理部12は、要求データDNaを受信してから要求データDNbを受信するまでの期間のみ識別情報付加部13を動作させることにより、当該識別情報付加部13におけるデータ処理負荷を低減し得るようになされている。

#### 【0036】

ところで送信処理部12の送信処理においては、送信装置2内のプログラム格納用メモリ（図示せず）に予め格納された所定の送信プログラムを送信装置2内におけるワークメモリ（図示せず）上に読み出して展開した送信装置2内のCPU（図示せず）と、当該送信処理部12とが協働して実現するようになされており、当該送信処理手順の説明については後述する。

#### 【0037】

##### （3）受信装置の構成

図5に示すように、パケット受信部22は、インターネット5（図1）及びインターフェイス（以下、これを受信側インターフェイスと呼ぶ）21を順次介してパケット（送信パケットPK、妨害対策パケットBMPK又は内容変更パケットFPK）を受信し、これを受信処理部23に与える。

#### 【0038】

受信処理部23の攻撃検出部24は、複数の送信装置からパケットを送信し始めるための所定のアクセスがあった際に予め当該送信装置との間で個々に使用セキュリティを決定し、各送信装置にそれぞれ対応する使用セキュリティを把握しておくようになされている。

#### 【0039】

従って攻撃検出部24は、パケット受信部22から与えられるパケットについて、当該パケットの送信元アドレスと、当該パケットに含まれるインデックス情報（SPI）とに基づいて当該パケットに用いられた使用セキュリティを検索し、当該検索した使用セキュリティに対応する例えば送信装置2を特定し得るようになされている。

**【0040】**

この状態において攻撃検出部 24 は、特定した送信装置 2 に対してサービス妨害対策の開始要求をしていない場合には、当該送信装置 2 から識別情報 J P が付加されない状態で送信される送信パケット P K に対して、第 1 のモード（以下、これを第 1 の攻撃検出モードと呼ぶ）でパケット復号処理を実行する。

**【0041】**

具体的に攻撃検出部 24 は、送信装置 2 から送信される送信パケット P K を、当該送信装置 2 に対応する使用セキュリティに従って復号する。

**【0042】**

ここで例えば本来得られるべきハッシュ値が得られない等の復号エラーが生じた場合には、攻撃検出部 24 は、送信装置 2 から送信された送信パケット P K の内容が変更された内容変更パケット F P Kであることを検出し、当該内容変更パケット F P K の本来の送信元が送信装置 2 であることをフィードバック制御部 25 に通知すると共に、当該内容変更パケット F P K を破棄する。

**【0043】**

これに対して攻撃検出部 24 は、送信パケット P K を復号した結果、送信パケット P K に含まれる暗号化データ片（図 3）を復元した場合には、当該データ片を送信装置 2 のデータ片として内部メモリに記憶する。

**【0044】**

一方、攻撃検出部 24 は、送信装置 2 にサービス妨害対策の開始要求をしている場合には、当該送信装置 2 から識別情報 J P が付加された状態で送信される妨害対策パケット B M P K（図 3）に対して、第 2 のモード（以下、これを第 2 の攻撃対策モードと呼ぶ）でパケット復号処理を実行する。

**【0045】**

具体的に攻撃検出部 24 は、当該送信装置 2 から送信される妨害対策パケット B M P K（図 3）の先頭に識別情報 J P が付加されているか否かを判定する。

**【0046】**

そして攻撃検出部 24 は、識別情報 J P が付加されている肯定結果が得られた場合には第 2 段階として、識別情報 J P のシーケンス番号 S（図 4）について、

予め内部メモリ（図示せず）に複数の送信装置単位で一旦記憶しておいた過去の識別情報 J P のシーケンス番号 S とは異なるか否かを判定する。

【0047】

さらに攻撃検出部 24 は、過去に受け取った識別情報 J P のシーケンス番号 S と異なっている肯定結果が得られた場合には第 3 段階として、送信装置 2 と同一の識別情報生成アルゴリズムにより、送信装置 2 と同一の種情報（シード）を用いて識別情報 J P と比較するための比較用識別情報を生成した後、当該識別情報 J P と比較用識別情報とを照合した結果が一致するか否かを判定する。

【0048】

ここで、第 1 段階で否定結果が得られた場合には、サービス妨害の開始を送信装置 2 に要求したにもかかわらず識別情報 J P が付加されていないので、送信パケット P K の内容を変更した不当な内容変更パケット F P Kであることを表わす。

【0049】

また第 2 段階又は第 3 段階で否定結果が得られた場合には、妨害対策パケット B M P K における内容に変更のある不当な内容変更パケット F P Kであることを表わす。

【0050】

従って攻撃検出部 24 は、第 1 段階、第 2 段階又は第 3 段階のいずれか 1 つでも否定結果が得られた場合には内容変更パケット F P Kであることを検出し、当該内容変更パケット F P K の本来の送信元が送信装置 2であることをフィードバック制御部 25 に通知すると共に、当該内容変更パケット F P Kを破棄する。

【0051】

これに対して攻撃検出部 24 は、第 1 段階、第 2 段階又は第 3 段階のいずれについても肯定結果が得られた場合には、当該送信装置 2 に対応する使用セキュリティに従って送信パケット P K を復号し、その結果復元されるデータ片を送信装置 2 のデータとして内部メモリに記憶する。

【0052】

このように攻撃検出部 24 は、第 1 の攻撃検出モードにおいて、パケット受信

部 2 2 から順次与えられるパケット毎に使用セキュリティを検索し、当該使用セキュリティに対応する送信装置を特定した後に復号することにより、正規の送信パケットに係るデータ片を複数の送信装置毎に内部メモリ上で管理すると共に、当該複数の送信装置毎に内容変更パケット F P K を検出し得るようになされている。

#### 【 0 0 5 3 】

また攻撃検出部 2 4 は、第 2 の攻撃検出モードにおいて、第 1 の攻撃検出モードと同様にして送信装置を特定した後に、送信パケット P K の先頭に未符号化状態で付加された識別情報 J P に基づいて内容変更パケット F P K であるか否かを判定することにより、当該送信パケット P K の復号前に複数の送信装置毎に内容変更パケット F P K を検出し得るようになされている。

#### 【 0 0 5 4 】

従って攻撃検出部 2 4 は、通信妨害装置 4 から大量の内容変更パケット F P K を受信した場合であっても、当該大量の内容変更パケット F P K をそれぞれ復号するまでもなく処理負荷の小さい簡易な処理によって破棄することができ、これにより受信装置 3 における処理負荷を格段に低減することができるようになされている。

#### 【 0 0 5 5 】

受信処理部 2 3 のフィードバック制御部 2 5 は、複数の送信装置ごとにカウンタを有し、攻撃検出部 2 4 から内容変更パケット F P K の本来の送信元である送信装置が通知される度に当該通知に対応する送信装置のカウンタを順次「1」ずつ繰り上げると共に、当該各カウンタにおける所定の単位時間当たりの繰り上げ数（以下、これを単位攻撃回数と呼ぶ）を内部クロックに基づいて計測する。

#### 【 0 0 5 6 】

かかる単位攻撃回数は、その数値が大きい場合には内容変更パケット F P K を大量に受信している、すなわちサービス妨害行為の規模が大きいことを表し、これに対して当該数値が小さい場合にはサービス妨害行為の規模が比較的小さいことを表す。

#### 【 0 0 5 7 】

またフィードバック制御部 25 は、カウンタの単位攻撃回数が所定の閾値よりも大きくなったとき、当該カウンタに対応する送信装置のサービス妨害対策の開始命令をフィードバック送信部 26 に与えると共に、当該送信装置に係るパケットを攻撃検出部 24 がパケット復号処理を実行する際に第 2 の攻撃対策モードで実行させる。

#### 【0058】

これに対してフィードバック制御部 25 は、カウンタの単位攻撃回数が所定の閾値よりも小さくなったとき、当該カウンタに対応する例えば送信装置のサービス妨害対策の停止命令をフィードバック送信部 26 に与えると共に、当該送信装置に係るパケットを攻撃検出部 24 がパケット復号処理を実行する際に第 1 の攻撃対策モードで実行させる。

#### 【0059】

かかる所定の閾値は、受信装置 3 の処理能力に応じて変更され、復号モードを実行する受信装置 3 が内容変更パケット FPK を大量に受けたことにより無駄に消費される処理負荷によって受信装置 3 が動作不能となってしまう単位攻撃回数のおよそ 10%～20% が選定される。

#### 【0060】

このようにフィードバック制御部 25 は、カウンタの単位攻撃回数に応じて攻撃検出部 24 における処理状態を切り換え得るようになされている。

#### 【0061】

フィードバック送信部 26 は、フィードバック制御部 25 から与えられる命令に応じた要求データ DN (DNa 又は DNb) を生成し、これを受信側インターフェイス 21 を介して例えば送信装置 2 (図 1) へ送信する。

#### 【0062】

かかる要求データ DN (DNa 及び DNb) としては、RFC (Request for Comments) と呼ばれる仕様書群のうち、例えば図 6 に示すように、RFC 792 において規定される ICMP (Internet Control Message Protocol) を適用するようになされている。

#### 【0063】



この場合、「code」には、「0」又は「1」が記述され、当該「1」であった場合にはサービス妨害対策の開始要求を表すと共に「0」であった場合にはサービス妨害対策の停止要求を表すようになされており、送信装置2では、当該「code」に記述された「0」又は「1」に基づいてサービス対策の開始又は停止要求を認識し得るようになされている。

#### 【0064】

因みに「type」には、受信装置3と受信装置2との間でそれぞれ認識し得る値が記述され、また「checksum」には、通信データDNが壊れているか否かを送信装置2がチェックするためのデータ列が記述されるようになされている。

#### 【0065】

このように受信処理部23は、複数の送信装置毎に内容変更パケットFPKをカウントして単位攻撃回数を計測し、当該計測結果が所定の閾値を上回ったとき又は下回った送信装置に対してのみ要求データDN（DNa及びDNb）を送信することにより、複数の送信装置のうち内容変更パケットFPKの本来の送信元である送信装置に対してのみサービス妨害対策を開始又は停止させ得るようになされている。

#### 【0066】

ところで受信処理部23の受信処理においては、送信プログラムに対応する受信プログラムが予め受信装置3内のプログラム格納用メモリ（図示せず）に格納されており、当該受信プログラムを受信装置3内におけるワークメモリ（図示せず）上に読み出して展開した受信装置3内のCPU（図示せず）と、受信処理部23とが協働して実現するようになされている。

#### 【0067】

以下、送信処理部12における送信処理手順と、受信処理部23における受信処理手順とをそれぞれフローチャートを用いて説明する。

#### 【0068】

（4）送信処理手順及び受信処理手順

（4-1）送信処理手順

まずは、送信処理部 12 における送信処理手順について図 7 に示すフローチャートを用いて説明する。

【0069】

すなわち送信処理部 12 は、例えば送信対象データ D1 を受信装置 3 へ送信する所定の送信操作が行われると、ルーチン R T 1 の開始ステップ S P 0 から次のステップ S P 1 へ移る。

【0070】

ステップ S P 1 において送信処理部 12 は、識別情報付加部 13 を妨害対策停止モードにし、次のステップ S P 2 へ移る。

【0071】

この場合、識別情報付加部 13 は休止状態にあり、従ってパケット生成部 11 から与えられる送信パケット P K は、識別情報 J P (図 4) を付加することなくそのまま送信側インターフェイス 15 に与えられる。

【0072】

ステップ S P 2 において送信処理部 12 は、フィードバック受信部 14 により、受信装置 3 (図 1) から送信される要求データ D N (D N a, D N b) を受信したか否かを判定する。ここで否定結果が得られると、このことは未だ要求データ D N を受信していないことを表しており、このとき送信処理部 12 は当該要求データ D N を受信するまで待ち受ける。

【0073】

これに対してステップ S P 2 で肯定結果が得られると、このことは要求データ D N を受信したことを表しており、このとき送信処理部 12 は、次のステップ S P 3 へ移る。

【0074】

ステップ S P 3 において送信処理部 12 は、フィードバック受信部 14 により、ステップ S P 2 で受信した要求データ D N のデータ内容に基づいて、受信装置 3 (図 1) がサービス妨害行為を受けているか否かを判定する。

【0075】

ここで肯定結果が得られると、このことは要求データ D N の「c o d e」 (図

6) に「1」が記述されている、すなわちサービス妨害対策の開始要求があったことを表しており、このとき送信処理部 12 は、次のステップ S P 4 へ移る。

【0076】

ステップ S P 4 において送信処理部 12 は、フィードバック受信部 14 により、識別情報付加部 13 を妨害対策停止モードから妨害対策モードに遷移させた後、ステップ S P 2 へ戻って、要求データ D N を受信するまで待ち受ける。

【0077】

この場合、識別情報付加部 13 は、パケット生成部 11 から与えられる送信パケット P K に識別情報 J P (図 4) を付加して妨害対策パケット B M P K (図 3) を生成し、当該妨害対策パケット B M P K を送信側インターフェイス 15 に与えるようになされている。

【0078】

一方、ステップ S P 3 で否定結果が得られると、このことは要求データ D N の「code」(図 6) に「0」が記述されている、すなわちサービス妨害対策の停止要求があったことを表しており、このとき送信処理部 12 は、次のステップ S P 5 へ移る。

【0079】

ステップ S P 5 において送信処理部 12 は、フィードバック受信部 14 により、識別情報付加部 13 が妨害対策モードである場合には、当該識別情報付加部 13 を妨害対策モードから妨害対策停止モードに遷移させた後、ステップ S P 2 へ戻って、要求データ D N を受信するまで待ち受ける。

【0080】

この場合、識別情報付加部 13 は再び休止状態となり、従ってパケット生成部 11 から与えられる送信パケット P K は、識別情報 J P (図 4) を付加することなくそのまま送信側インターフェイス 15 に与えられるようになされている。

【0081】

(4-2) 受信処理手順

次に、受信処理部 23 における受信処理手順について図 8 に示すフローチャートを用いて説明する。

**【 0 0 8 2 】**

すなわち受信処理部 2 3 は、ルーチン R T 2 の開始ステップ S P 1 0 から次のステップ S P 1 1 へ移る。

**【 0 0 8 3 】**

ステップ S P 1 1 において受信処理部 2 3 は、攻撃検出部 2 4 により、パケット（送信パケット P K 又は内容変更パケット F P K）を受け取ったか否かを判定する。

**【 0 0 8 4 】**

ここで否定結果が得られると、このことは未だパケット受信部 2 2 がパケット受信していないことを表しており、このとき受信処理部 2 3 は、当該パケットを受け取るまで待ち受ける。

**【 0 0 8 5 】**

これに対して肯定結果が得られると、このことはパケット受信部 2 2 がパケットを受信したことを表しており、このとき受信処理部 2 3 は、次のステップ S P 1 2 へ移る。

**【 0 0 8 6 】**

ステップ S P 1 2 において受信処理部 2 3 は、ステップ S P 1 1 で受け取ったパケットに基づいて、当該パケットの送信元である例えば送信装置 2 を特定し、次のステップ S P 1 3 へ移る。

**【 0 0 8 7 】**

ステップ S P 1 3 において受信処理部 2 3 は、攻撃検出部 2 4 により、ステップ S P 1 2 で特定した送信装置 2 に対してサービス妨害対策を停止させている場合には第 1 の攻撃検出モードでパケット復号処理を実行し、これに対してサービス対策を開始させている場合には第 2 の攻撃検出モードでパケット復号処理を実行し、ステップ S P 1 1 で受け取ったパケットが内容変更パケット F P K であるか否かを判定する。

**【 0 0 8 8 】**

ここで否定結果が得られると、このことはステップ S P 1 1 で受け取ったパケットについては、送信装置 2（図 1）から送信された正当な送信パケット P K 又

は妨害対策パケットBMPKであることを表しており、このとき受信処理部23は、攻撃検出部24により当該送信パケットPK又は妨害対策パケットBMPKに含まれるデータ片を送信装置2のデータ片として内部メモリに記憶した後、ステップSP11に戻って再びパケットを受信するまで待ち受ける。

#### 【0089】

これに対してステップSP13で肯定結果が得られると、このことはステップSP11で受け取ったパケットが実際には通信妨害装置4（図1）から送信された不当な内容変更パケットFPKであることを表しており、このとき受信処理部23は、次のステップSP14へ移る。

#### 【0090】

ステップSP14において受信処理部23は、攻撃検出部24により、ステップSP13で判定した内容変更パケットFPKを破棄すると共に、内容変更パケットFPKの生成元が送信装置2であることをフィードバック制御部25に通知した後、次のステップSP15へ移る。

#### 【0091】

ステップSP15において受信処理部23は、フィードバック制御部25により、攻撃検出部24から通知された、すなわちステップSP12で特定した送信装置2に対応するカウンタを「1」つ分だけ繰り上げ、次のステップSP16へ移る。

#### 【0092】

ステップSP16において受信処理部23は、ステップSP15で繰り上げたカウンタを計測する単位攻撃回数（単位時間当たりの繰り上げ数）が所定の閾値を越えているか否かを判定する。

#### 【0093】

ここで肯定結果が得られると、このことは送信装置2から送信されたパケット（送信パケットPK又は妨害対策パケットBMPK）の送信アドレス等が書き換えられて生成された内容変更パケットFPKの受信量が多く、すなわちサービス妨害行為の規模が大きいことを表しており、このとき受信処理部23は、次のステップSP17へ移る。

**【0094】**

ステップSP17において受信処理部23は、送信装置2にサービス妨害対策を停止させていた場合には、フィードバック送信部26によりサービス妨害対策の開始を要求する要求データDNaを生成して受信側インターフェイス21を介して送信装置2へ送信した後、ステップSP11に戻る。

**【0095】**

これに対してステップSP16で否定結果が得られると、このことは送信装置2から送信されたパケット（送信パケットPK又は妨害対策パケットBMPK）の送信アドレス等が書き換えられて生成された内容変更パケットFPKの受信量が少なくなった又は全くない、すなわちサービス妨害行為の規模が小さくなった又はサービス妨害行為が行われていないことを表しており、このとき受信処理部23は、次のステップSP18へ移る。

**【0096】**

ステップSP18において受信処理部23は、送信装置2にサービス妨害対策を開始させていた場合には、フィードバック制御部25により送信装置2に対応するカウンタをリセットすると共に、フィードバック送信部26によりサービス妨害対策の停止を要求する要求データDNbを生成して受信側インターフェイス21を介して送信装置2へ送信した後、ステップSP11に戻る。

**【0097】**

因みに受信処理部23は、ステップSP17において送信装置2にサービス妨害対策を既に開始させていた場合、及びステップSP18において送信装置2にサービス妨害対策を既に停止させていた場合には何ら処理することなくステップSP11へ戻るようになされている。

**【0098】****(5) 動作及び効果**

以上の構成において、送信装置2は、送信手段としての送信側インターフェイス15により、IPsecに規定される暗号プロトコルに準拠して生成された送信パケットPKを順次インターネット5を介して送信する。

**【0099】**

この状態において送信装置 2 は、識別情報付加手段としての識別情報付加部 13 により、送信パケット P K の送信対象である受信装置 3 から要求があった期間（すなわち要求データ D N a を受けてから当該要求データ D N b を受けるまでの期間）のみ識別情報 J P を送信パケット P K に付加するようにした。

#### 【0100】

この場合、送信装置 2 は、受信装置 3 から要求がない場合に識別情報 J P を送信パケット J P に付加して送信しない分だけ送信装置 2 自身及びインターネット 5 上におけるルータ等の中間ノードに対する処理負荷を低減することができる。

#### 【0101】

また送信装置 2 は、受信装置 3 から要求があった期間以外は休止状態にあるようにしたことにより、当該受信装置 3 から要求がない場合に識別情報 J P を生成しない分だけ識別情報付加部 13 自身の処理負荷を低減できると共に省電力化を図ることができる。

#### 【0102】

一方、受信装置 3 は、受信手段としての受信側インターフェイス 21 により、送信装置 2 からインターネット 5 を介して順次送信された送信パケット P K（妨害対策パケット B M P K）を受信し、検出手段としての攻撃検出手段 24 により、当該受信した各送信パケット P K のうち、当該パケットの内容が変更された送信パケットである内容変更パケット F P K を検出する。

#### 【0103】

この状態において受信装置 3 は、要求手段としてのフィードバック制御部 25 及びフィードバック送信部 26 により、検出された内容変更パケット F P K の単位攻撃回数が所定の閾値よりも上回っているときのみ識別情報 J P の送信パケット P K への付加を送信装置 2 に要求するようにした。

#### 【0104】

この場合、受信装置 3 は、送信装置 2 に要求しない際に送信装置 2 からは識別情報 J P の付加された妨害対策パケット B M P K が送信されない分だけ送信装置 2 自身及びインターネット 5 上におけるルータ等の中間ノードに対する処理負荷を低減することができる。

**【0105】**

ここで、受信装置3は、送信装置2と受信装置3とだけが独自に有する識別情報生成アルゴリズムに従って擬似乱数Gと、当該擬似乱数Gに対して固有なシーケンス番号Sとでなる識別情報JPに基づいて内容変更パケットFPKであるか否かを判定することにより、当該識別情報JPの有無を認識する（第1段階）、或いは単に過去のシーケンス番号Sとの同一性や擬似乱数列Gとの同一性の照合するだけで内容変更パケットFPKを検出することができる。

**【0106】**

この場合、受信装置3は、送信パケットPKの復号の際に内容変更パケットFPKを検出する場合に比して処理負荷の小さい簡易な処理で当該内容変更パケットFPKを検出することができ、これにより通信妨害装置4から大量の内容変更パケットFPKを受信した場合であっても、処理負荷を格段に低減することができる、その結果、大量の内容変更パケットFPKを受信したことによるシステムダウン等を防止することができる。

**【0107】**

また受信装置3は、複数の送信装置のうち、内容変更パケットFPKに係る送信パケットPKを送信する送信装置2に対してのみ識別情報JPの付加を要求するようにしたことにより、当該複数の送信装置全てに対して要求する場合に比してインターネット5上における処理負荷を格段に低減することができる。

**【0108】**

以上の構成によれば、当時装置である正規の送信装置2と受信装置3との間で複数の送信パケットPKをインターネット5を介して送受信中に、当該受信装置3に送信される内容変更パケットFPKの単位攻撃回数が所定の閾値を上回っているときだけ当該各送信パケットPKにそれぞれ識別情報JPを付加した妨害対策パケットBMPKを送受信するようにしたことにより、サービス妨害行為がなかった場合には各送信パケットPKにそれぞれ識別情報JPを付加しない分だけ送信装置2、インターネット5上の中間ノード及び受信装置3における送受信システム1全体の処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。



## 【0109】

## (6) 他の実施の形態

上述の実施の形態においては、受信装置3が受信した内容変更パケットF P Kの単位攻撃回数が所定の閾値を上回ったときサービス妨害対策の開始を行わせるようにした場合について述べたが、本発明はこれに限らず、当該受信装置を統括的に制御するC P Uの処理負荷を常時監視し、当該C P Uの処理負荷が所定の閾値を上回ったときサービス妨害対策の開始を行わせる等、要は、受信装置3における受信状況に応じてサービス妨害対策の開始を行わせるようにすることができる。

## 【0110】

さらに上述の実施の形態においては、図6について上述した構成の要求データD Nを適用する場合について述べたが、本発明はこれに限らず、この他種々の構成でなる要求データを本発明を適用することができる。

## 【0111】

さらに上述の実施の形態においては、要求データD Nを送信パケットP Kと同一のネットワークであるインターネット5を介して送信するようにした場合について述べたが、本発明はこれに限らず、要求データD Nと送信パケットP Kとをそれぞれ異なるネットワークを介して送受信するようにしても良く、要は、受信装置3が識別情報J Pの送信パケットP Kへの付加を送信装置2に要求した際に、当該要求に送信装置2が応じるような要求手法を選定することができる。

## 【0112】

さらに上述の実施の形態においては、インターネット5上の通信プロトコルであるI P sec に本発明を適用する場合について述べたが、本発明はこれに限らず、例えばS S H等のインターネット上の通信プロトコル、L A N (Local Area Network) 上の通信プロトコル、衛星放送上の通信プロトコル又は文字放送上の通信プロトコル等、他のネットワーク上におけるこの他種々の通信プロトコルに本発明を適用することができる。

## 【0113】

さらに上述の実施の形態においては、送信処理部12 (図2) における送信処

理を送信プログラムによって実現すると共に、受信処理部 23（図 3）における受信処理を受信プログラムによって実現するようにした場合について述べたが、本発明はこれに限らず、当該送信装置 2 内の各部全体の処理を当該送信プログラムによって実現するようにしても良く、また受信装置 3 内の各部全体の処理を当該受信プログラムによって実現するようにしても良く、当該各部をそれぞれ専用の集積回路によって実現するようにしても良い。

#### 【0114】

さらに上述の実施の形態においては、プログラム格納用メモリ内に予め格納された送信プログラムに従って図 7 について上述した送信処理手順で送信処理を実行すると共に、当該メモリ内に予め受信プログラムに従って図 8 について上述した受信処理手順で受信処理を実行するようにした場合について述べたが、本発明はこれに限らず、送信プログラム及び又は受信プログラムが格納されたプログラム格納媒体から情報処理装置にインストールすることにより当該送信処理及び又は受信処理を実行するようにしても良い。

#### 【0115】

この場合、かかる送信プログラム及び又は受信プログラムを情報処理装置にインストールして実行可能な状態にするためのプログラム格納媒体としては、例えばフレキシブルディスク、CD-ROM（Compact Disk-Read Only Memory）、DVD（Digital Versatile Disc）等のパッケージメディアのみならず、プログラムが一時的若しくは永続的に格納される半導体メモリや磁気ディスク等で実現しても良い。またこれらプログラム格納媒体に送信プログラム及び又は受信プログラムを格納する手段として、ローカルエリアネットワークやインターネット、デジタル衛星放送等の有線又は無線通信媒体を利用しても良く、ルータやモデム等の各種通信インターフェースを介して格納するようにしても良い。

#### 【0116】

##### 【発明の効果】

上述のように本発明によれば、所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信し、当該送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別

情報を各送信パケットに付加するようにしたことにより、受信側から要求があった期間以外については識別情報を各送信パケットに付加しない分だけ送信手段、識別情報付加手段及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。

#### 【0117】

また、上述のように本発明によれば、送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信し、当該受信された各送信パケットのうち、当該パケットの内容が変更された送信パケットである内容変更パケットを検出し、当該検出した内容変更パケットの受信状況に応じて、検出手段だけに識別させるための識別情報の送信パケットへの付加を送信側に要求するようにしたことにより、送信側に要求しない際に送信側からは識別情報の付加された送信パケットが送信されない分だけ送信装置及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。

#### 【図面の簡単な説明】

##### 【図1】

本発明を適用した送受信システムの全体構成を示す略線図である。

##### 【図2】

送信装置の構成を示すブロック図である。

##### 【図3】

妨害対策パケットの構成を示す略線図である。

##### 【図4】

識別情報の構成を示す略線図である。

##### 【図5】

受信装置の構成を示すブロック図である。

##### 【図6】

要求データの構成を示す略線図である。

##### 【図7】

送信処理手順を示すフローチャートである。

【図 8】

受信処理手順を示すフローチャートである。

【符号の説明】

1 ……送受信システム、2 ……送信装置、3 ……受信装置、4 ……通信妨害装置、1 2 ……送信処理部、1 3 ……識別情報付加部、1 4 ……フィードバック受信部、2 4 ……攻撃検出部、2 5 ……フィードバック制御部、2 6 ……フィードバック送信部。

【書類名】 図面

【図 1】

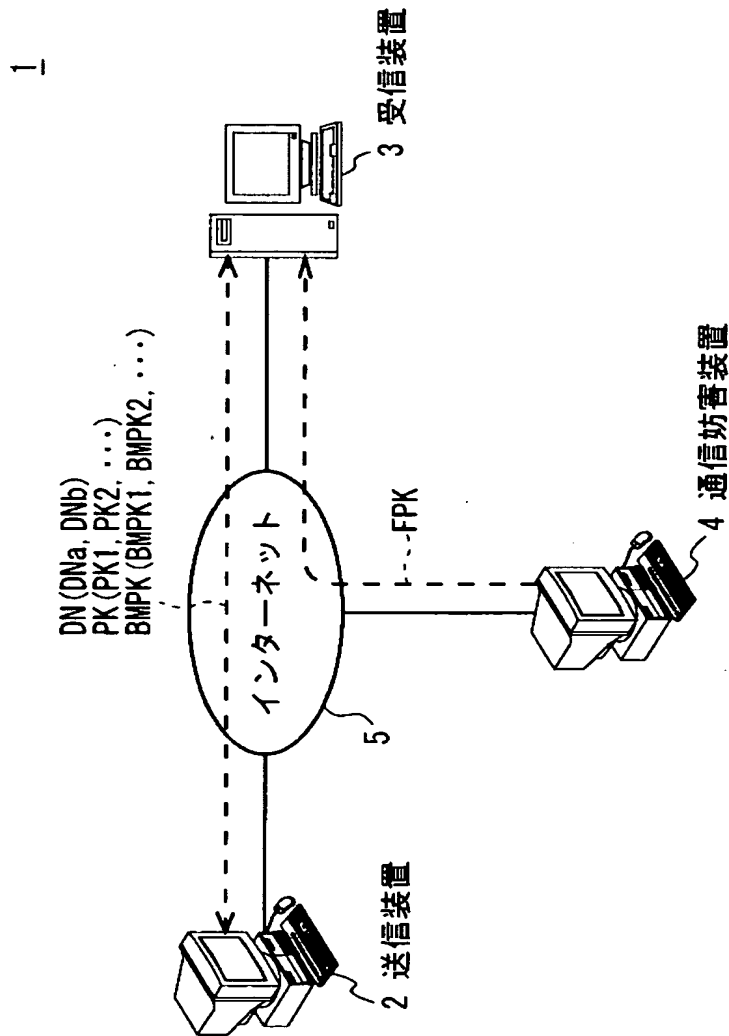


図 1 送受信システムの全体構成

【図 2】

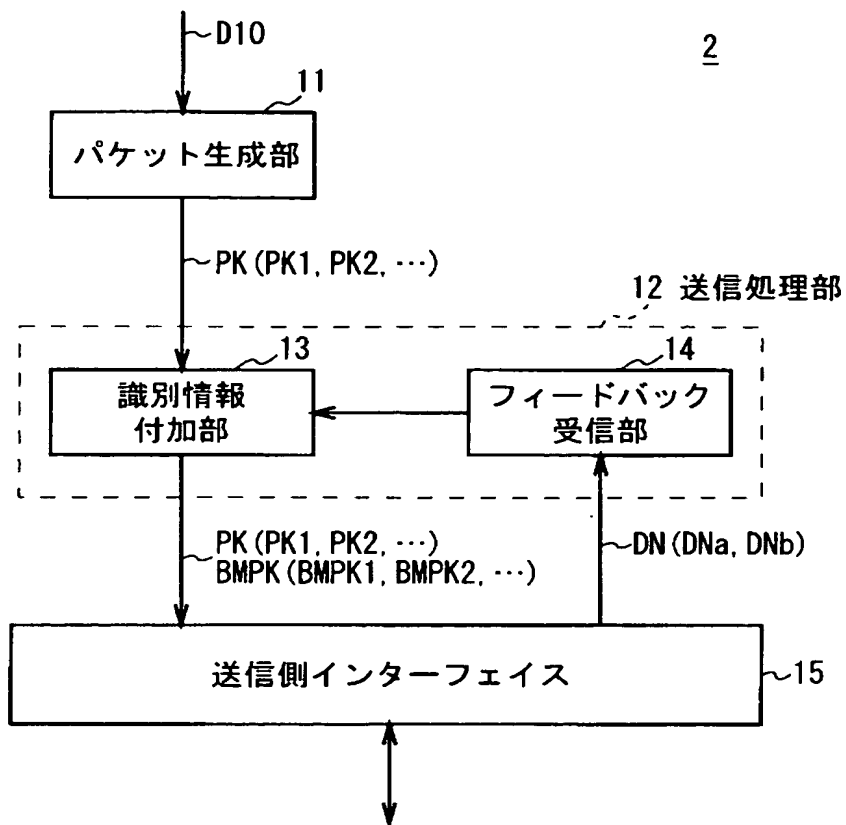


図 2 送信装置の構成

【図 3】

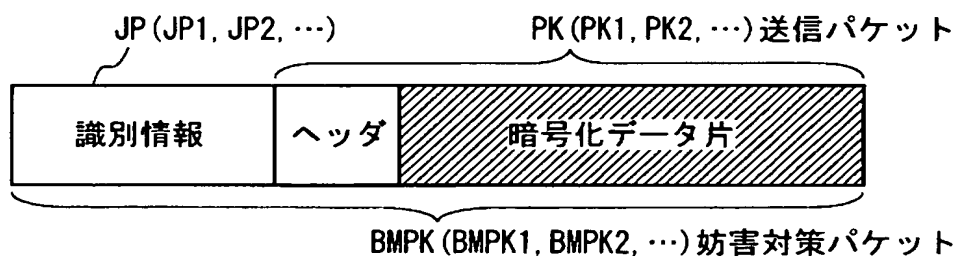


図 3 妨害対策パケットの構成

【図 4】

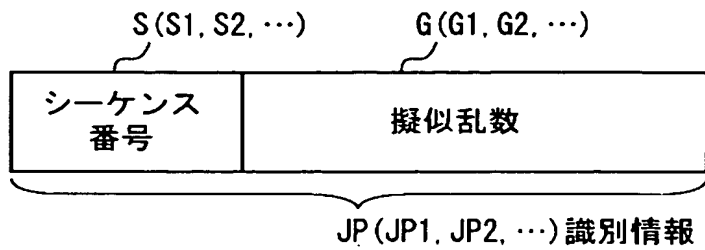


図 4 識別情報の構成

【図 5】

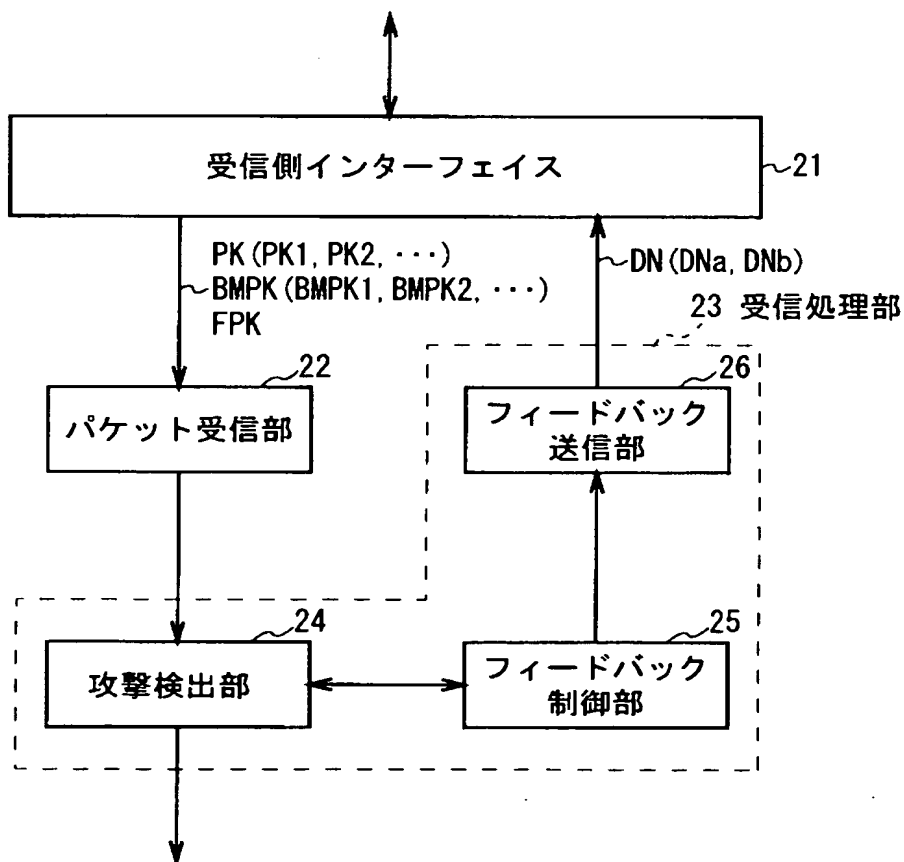
3

図 5 受信装置の構成

【図 6】

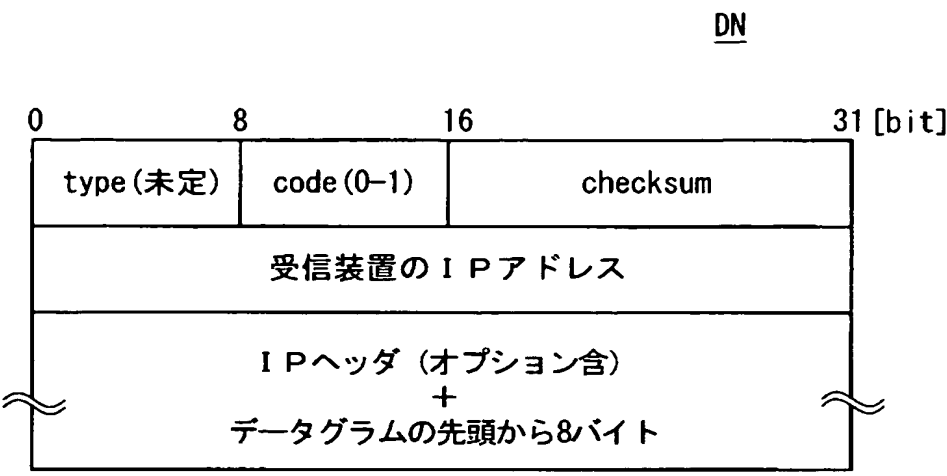


図 6 要求データの構成



【図 7】

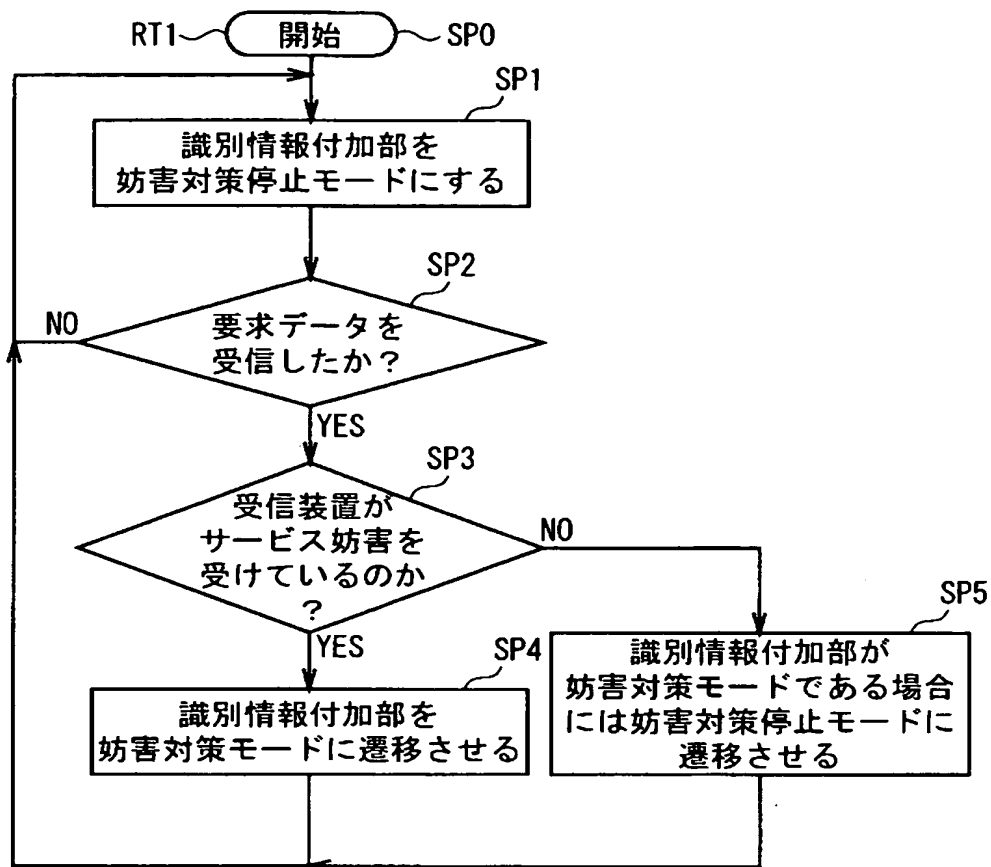


図 7 送信処理手順

【図 8】

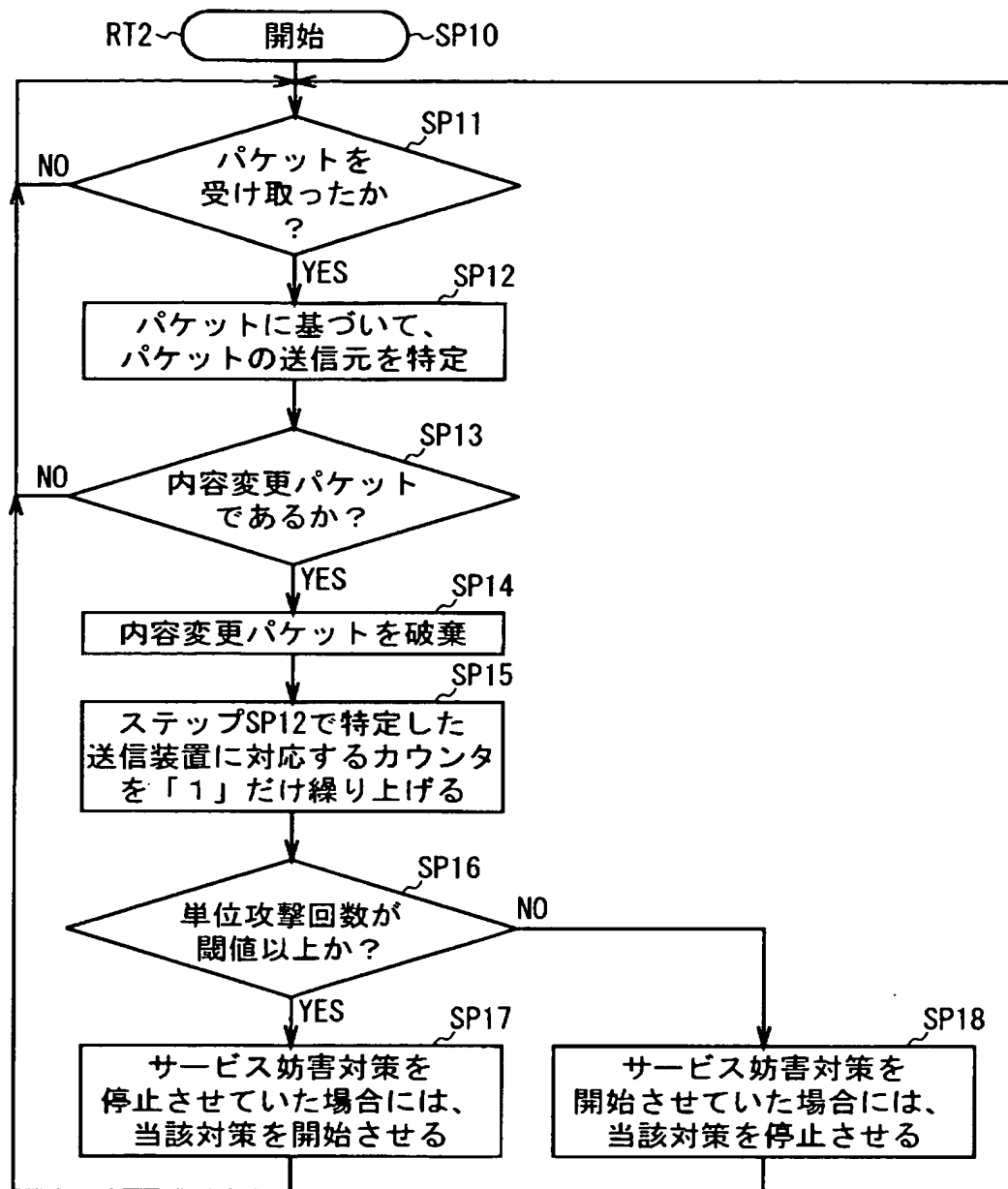


図 8 受信処理手順

【書類名】 要約書

【要約】

【課題】

本発明は、システム全体としての送信効率を向上できるようにする。

【解決手段】

本発明は、正規の送信装置 2 と受信装置 3 との間で複数の送信パケット P K をインターネット 5 を介して送受信中に、当該受信装置 3 に送信される内容変更パケット F P K の単位攻撃回数が所定の閾値を上回っているときだけ当該各送信パケット P K にそれぞれ識別情報 J P を付加した妨害対策パケット B M P K を送受信することにより、サービス妨害行為がなかった場合には各送信パケット P K にそれぞれ識別情報 J P を付加しない分だけ送信装置 2、インターネット 5 上の中間ノード及び受信装置 3 における処理負荷を低減することができ、かくして、送受信システム 1 全体としての送信効率を向上することができる。

【選択図】 図 1

特願 2 0 0 3 - 0 1 6 6 4 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日  
[変更理由]

1 9 9 0 年 8 月 3 0 日  
新規登録

住 所  
氏 名

東京都品川区北品川 6 丁目 7 番 3 5 号  
ソニー株式会社